Defense Information Systems Agency

A Combat Support Agency

Enterprise User

"I can go anywhere in the DoD, login, and be productive."

Common User Services

The "Cloud" and the Future of DOD IT

COMMERCIAL CLOUD COMPUTING

DISA
A Combat Support Agency

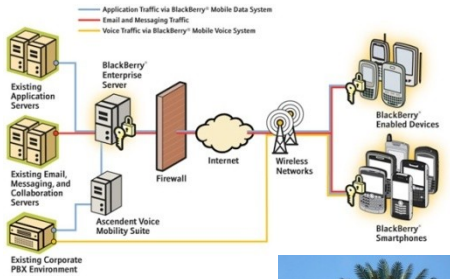
View = *Angry Birds!*

- ***Angry Birds!*** (it's a game)
  - User Applications
  - **Software as a Service (SaaS)**
  - Abstracts the Platform

*

Windows phone
iOS
android

- ***Android, iOS, Windows, etc.***
  - Operating system, identity & access control, basic apps, etc.
  - **Platform as a Service (PaaS)**



- ***Verizon, AT&T, etc.***
  - Smart Phone Network
  - Abstracts the Infrastructure
  - **Infrastructure as a Service (IaaS)**
  - Abstracts processing, storage, networking, security, etc.

***NOTE:** *The end-user hardware itself is not part of the Cloud Computing concept*

DISA
A Combat Support Agency

DOD CLOUD COMPUTING

DOD Component View = Outsourcing

- **Cloud Computing = Outsourcing of IT**
- **Allows DOD Components to**
- **Devote personnel to DOD Component missions**
- **Reduce costs**
- **Improve IT capabilities and speed of delivery**
- **Outsourcing to commercial cloud problematic for DOD**

"Most government agencies, financial institutions and some areas of medical services might never buy into true cloud computing because, at the end of the day, they need to know that all of their data in Richmond, Va., or Toledo, Ohio, is resting comfortably in a secure location that they can access at any time."*

- **Logical course for DOD Components is to outsource to a government cloud = the DOD Community Cloud**
  - **DISA is the logical provider**

**5 Technologies That Will Change the Market: What You Need to Know to Survive the Disruptions Ahead,* Carlos A. Soto, Washington Technology, Aug 02, 2010.

DOD COMMUNITY CLOUD
DISA View = Layered Services

A Combat Support Agency

This is the Community Cloud DISA is providing

DISA Software as a Service (SaaS)
- User Applications
- Managed Services

App A	App B	App C	App etc

Other Software as a Service (SaaS)
- User Applications

App 1	App 2	App 3	App etc

DISA Platform as a Service (PaaS)
- Operating Systems
- Identity & Access Control Services
- File System, development & testing

Other Platform as a Service (PaaS)
- Operating Systems
- Identity & Access Control Services
- File System

DISA Infrastructure as a Service (IaaS)
- Processing, Storage, & Memory
- Security Services
- Network Transport

DOD CLOUD COMPUTING
User's View = Enterprise User

DISA
A Combat Support Agency

"I can go anywhere in the DOD, login, and be productive."

"I never have to make up a username, because its always the same everywhere – NIPR & SIPR."

"My CAC works at any base I go to – I just put it in a DoD computer and get an account."

Enterprise User

•Enterprise Identity
- Persona Username, Display Name & E-Mail Address (FY11)
- Enterprise Authentication and Access Control (FY11)

•DoD Visitor
- Automatic account provisioning on any NIPR computer
- Being installed on all DoD domain controllers now
- NIPR (FY11) and SIPR (FY12)

"I can always be sure people can find me because there's just one place to enter my info."

"Wherever I am, I can get to my e-mail, files & content, use office apps and find people."

•Enterprise User Data
- Personnel Portal at DMDC (FY11)
- Enterprise Identity & Contact Data Synchronization (FY11)

•Basic Web Services
- E-Mail (FY11)
- SharePoint (FY12)
- Office Web Applications (FY12)
- Directory Services (GAL & White Pages) (FY12)
- File Storage Service (*MyStuff*) (FY12)
- Content Management Service (FY12)

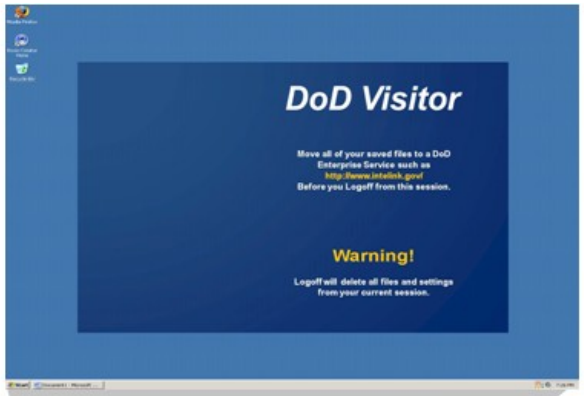
DOD Visitor System

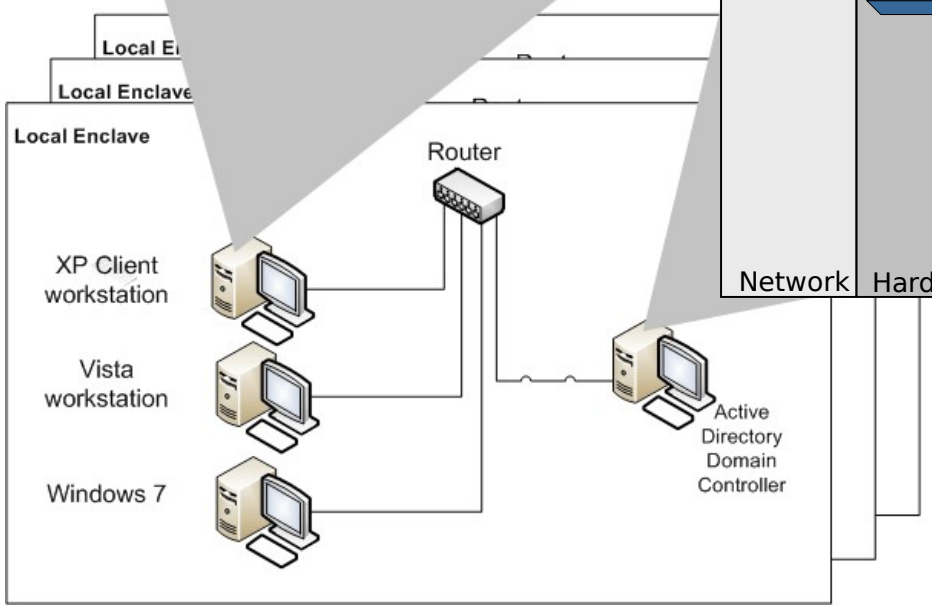
- DOD-wide implementation in FY11
- Mandated by CYBERCOM CTO

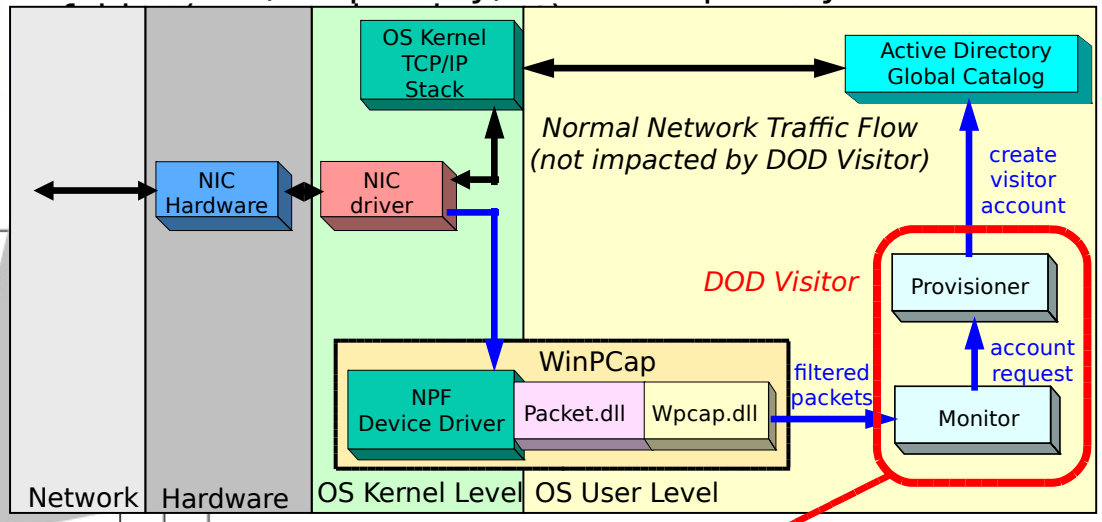
A Combat Support Agency

- DOD Visitor is installed on local Domain Controllers
- Nothing is installed on the Workstation
- Using Valid CAC → automatically get users account on any DoD NIPRNET computer
- User applications are "white listed"
  - Restricted to *Internet Explorer*, *Word*, *Excel*, *PowerPoint*, *Adobe Reader* and local print
  - User cannot execute other programs, or use CD/DVDs or flash drives
- Store files (temporarily) on desktop or My Documents

Visiting User Desktop







Monitor / Provisioner Code

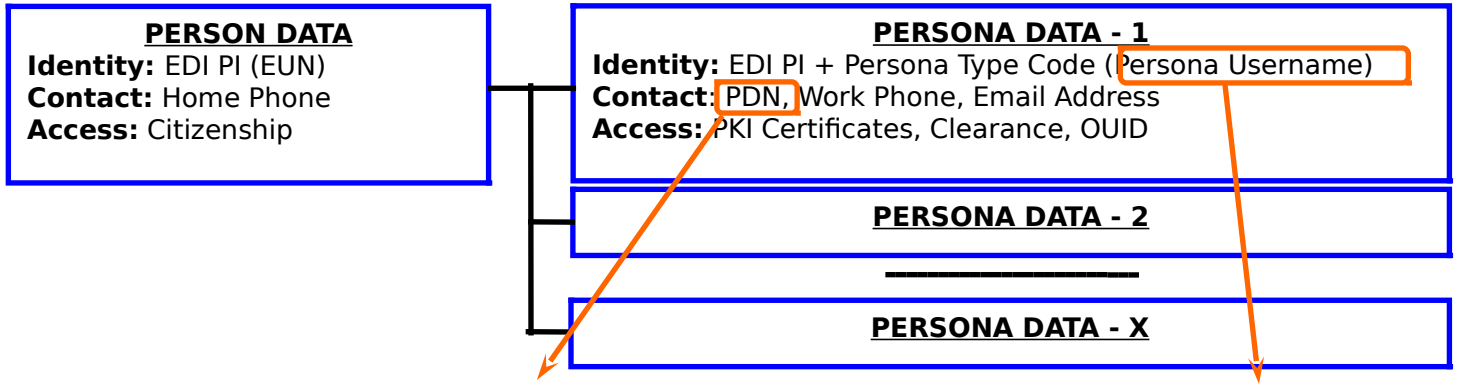
+

Group Policy Object (GPO) to restrict user capabilities

(GPOs are a standard component of Active Directory)

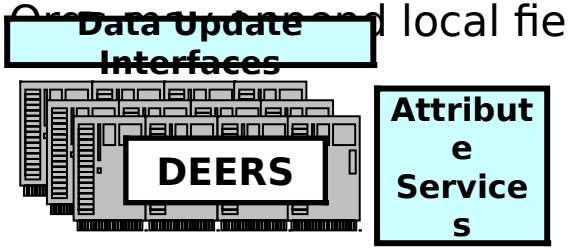
Enterprise Identity & Enterprise User Data

A Combat Support Agency


PERSON DATA
Identity: EDI PI (EUN)
Contact: Home Phone
Access: Citizenship
PERSONA DATA - 1
Identity: EDI PI + Persona Type Code (Persona Username)
Contact: PDN, Work Phone, Email Address
Access: PKI Certificates, Clearance, OUID
PERSONA DATA - 2
PERSONA DATA - X

"Smith, John E CAPT USN PACOM MIL (US)"

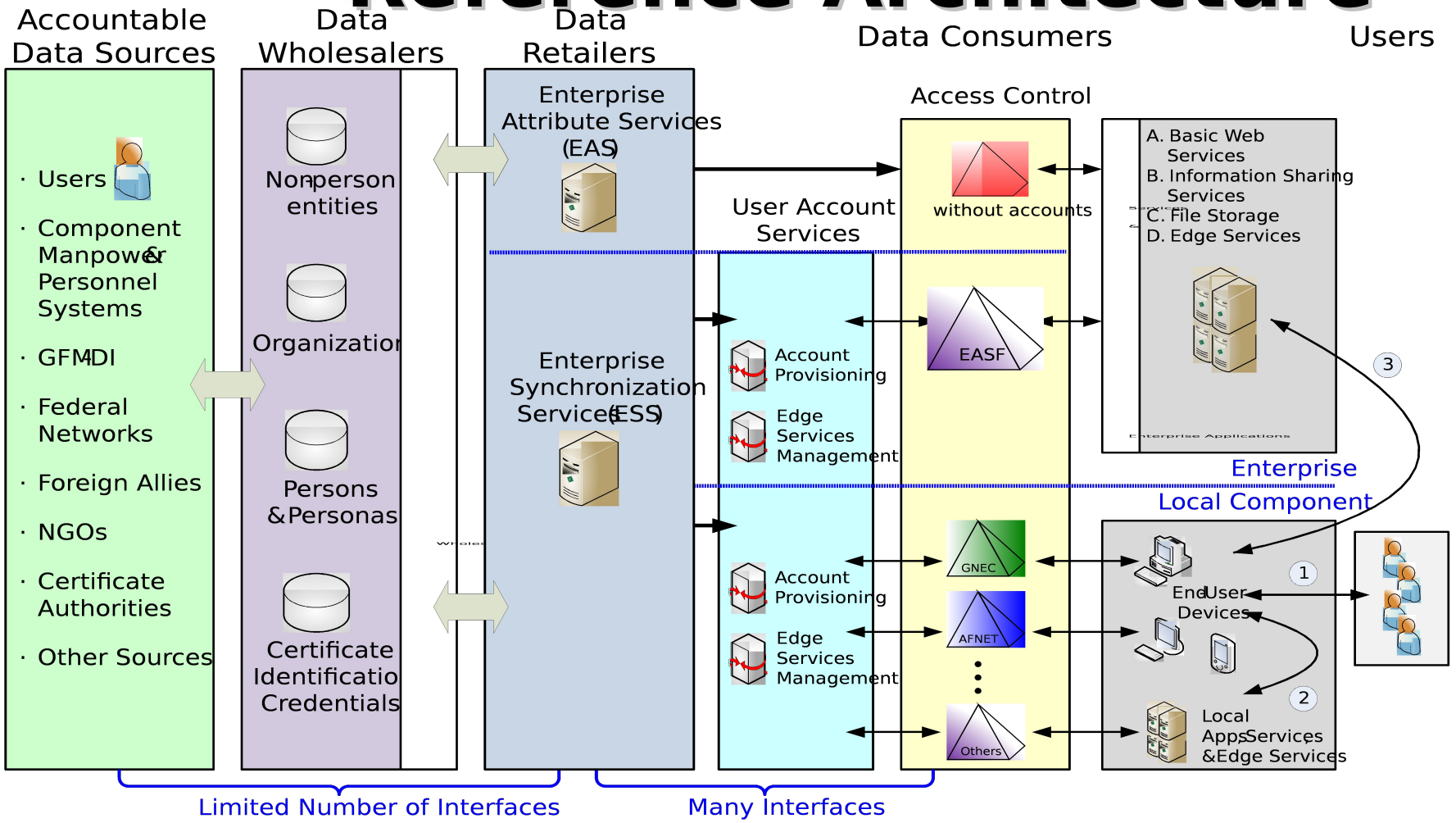
- DOD Persona Display Name (PDN)
  - Persona based
  - Changes as data changes
  - Data from DMDC
  - Implemented by DMDC in FY10
  - Mandatory when accounts with display names used (such as DCO, E-Mail)
  - Org, Type and local fields



"john.e.smith34.mil"

- DOD Persona Username (PUN) – (EUN) + Persona Extension
- Persona based
- Permanently assigned (assigned another if name changed)
- Data from DMDC
- Implemented by DMDC – Apr 10
- Seeded from AKO/DKO and NMCI
- Mandatory when accounts used
  - One account per Persona
- Access control will need to convert from Person-based to Persona-based

Enterprise User Reference Architecture*



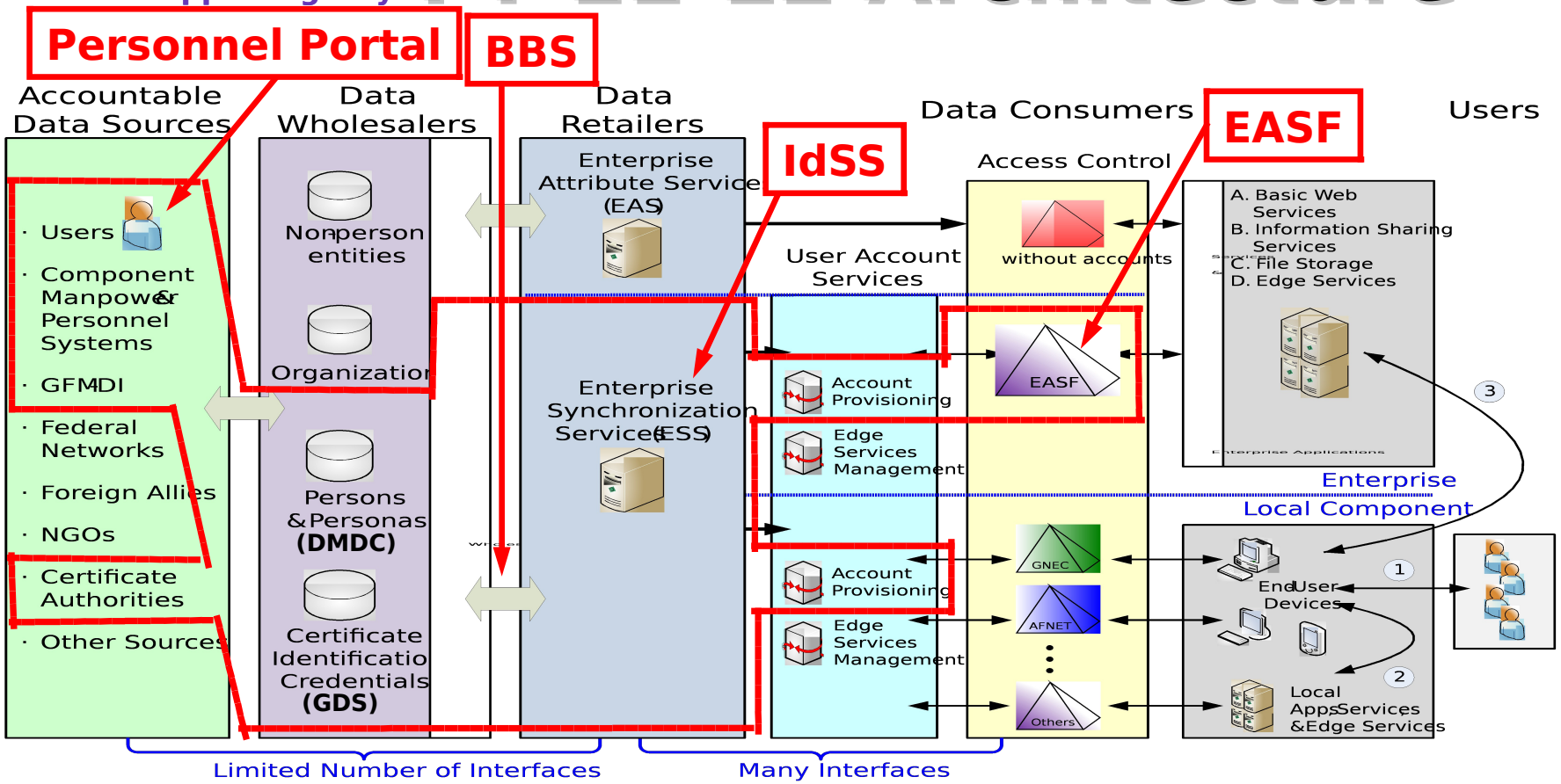
A. Basic Web Services: E-Mail, White Pages, Office Automation, etc
B. Information Sharing Services: Search, Collaboration, Wikis, Blogs, etc
C. File Storage: For Individuals and Organizations
D. Edge Services: Replication for disconnected operations

1. End-User device access
2. Access to Local Application
3. Access to Enterprise Servi

* **Architecture based on *Enterprise User Data Management Plan for Persons and Personas* (approved by DoD CIO, DMDC, & DISA)**

Identity & Access Control FY 11-12 Architecture

A Combat Support Agency



A. Basic Web Services: E-Mail, White Pages, Office Automation, etc
B. Information Sharing Services: Search, Collaboration, Wikis, Blogs, etc
C. File Storage: For Individuals and Organizations
D. Edge Services: Replication for disconnected operations

1. End-User device access
2. Access to Local Applicatior
3. Access to Enterprise Servi

← indicates Identity Synchronization, and Account Provisioning & Access Control components being implemented now;
other components in various stages of planning and/or implementation

DMDC – Defense Manpower Data Center; **BBS** – Batch Broker Service; **IdSS** – Identity Synchronization Service;
EASF – Enterprise Application and Support Forest; **GNEC** – Army Global Network; **AFNET** – Air Force

DISA
A Combat Support Agency

Basic Web Services

- **Deploy related capabilities together in Pods**
  - **Enterprise Application Service Forest (EASF)**
  - **Exchange Enterprise E-Mail**
  - **Enterprise SharePoint Service (ESPS)**
  - **Enterprise Directory Services (GAL & White Pages)**
  - **User storage for generic purposes (“MyStuff”)**
    - **Hierarchical file system**
    - **Access from duty station and remote**
  - **Enterprise Content Management**
  - **Other new (but related) capabilities**
- **Storage – full de-duplication on primary storage without archiving**

DISA DOD Common User Services

A Combat Support Agency

"I can go anywhere in the DOD, login, and be productive."

"I never have to make up a username, because its always the same everywhere – NIPR & SIPR."

"My CAC works at any base I go to – I just put it in a DoD computer and get an account."

•Enterprise Identity

- Persona Username, Display Name & E-Mail Address (FY11)
- Enterprise Authentication and Access Control (FY11)

Enterprise User

•DoD Visitor

- Automatic account provisioning on any NIPR computer
- Being installed on all DoD domain controllers now
- NIPR (FY11) and SIPR (FY12)

"I can always be sure people can find me because there's just one place to enter my info."

"Wherever I am, I can get to my e-mail, files & content, use office apps and find people."

•Enterprise User Data

- Personnel Portal at DMDC (FY11)
- Enterprise Identity & Contact Data Synchronization (FY11)

•Basic Web Services

- E-Mail (FY11)
- SharePoint (FY12)
- Office Web Applications (FY12)
- Directory Services (GAL & White Pages) (FY12)
- File Storage Service (*MyStuff*) (FY12)
- Content Management Service (FY12)

DEFENSE INFORMATION SYSTEMS AGENCY